UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,147	03/14/2001	Takahiro Nagai	2001-0295A	1782

513 7590 04/21/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/805,147	NAGAI ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/03/2004 (Amendment)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's argument, see "Kori and Wehrenberg fail to disclose or suggest a data signal having superimposed thereto, as a digital watermark, identification data identifying the data signal as an encrypted signal", filed February 23, 2004, with respect to the rejection(s) of claim(s) 1-9,13-15, 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Kori et al (US 6,480, 607 B1) have been fully considered and are persuasive. Claim(s) 10-12, 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kori, and further in view of Wehrenberg (US 6,523,113 B1) have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made herein.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-9,13-15, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kori, further in view of Ezaki et al (US 6,721,437 B1).

a. *Referring to claim 1:*

i. Kori teaches:

(1) An encrypted data signal comprising an encrypted copy-controlled data signal, wherein the data signal contains superimposed thereto, as a digital watermark, identification data identifying the data signal as an encrypted signal **[i.e., referring to Figure 6, to the third CSS decoder 51, control data for copyright control is sent from the data processing device 60 via an input interface, not shown. This control data is already encrypted using algorithms or encryption keys different from those for the picture data etc and the media type information. In a data area of an optical disc D is recorded picture data on moving or still**

pictures or speech data on music or speech. These data are previously compressed in accordance with the MPEG system. On the picture data, the copyright information is superimposed by the above-mentioned watermark processing (column 12, lines 21-41). Furthermore, the WM detection unit 61 is fed with picture data expanded by the MPEG decoder 21. The WM detection unit 61 detects (which means identifies) the encrypted key superimposed on the picture data by watermark processing to send the detected encrypted key to the encrypting unit 62. The encrypting unit 62 is fed with the pass information of the ticket from the ticket verification unit 22. The encrypting unit 62 encrypts the ticket pass information using the above-mentioned encrypting key. The encrypted ticket pass information is sent to the VID encoder 41. In addition, the ticket information, encrypted as the VID during the blanking period, is superimposed on the video signals (these are the encrypted signals) (column 16, lines 10-34)].

ii. Although Kori transparently and implicitly teaches identification data identifying the data signal as an encrypted signal as mention above, Exaki et al teaches:

(1) The encryption section 142 of the transmission side apparatus 140 encrypts original contents S0 using such a key as described above. The original contents S0 may be, for example, a video signal and/or an audio signal or the like. When the encryption section 142 encrypts the original contents S0, it also encrypts CCI (Copy Control Information) indicative of whether or not copying of an audio signal illustrated in FIG. 2 or a video signal illustrated in FIGS. 3A and 3B is inhibited and places the encrypted CCI into the encrypted signal of the original contents S0. Accordingly, the encryption signal SE includes not only the encrypted original contents S0 but also the encrypted CCI which indicates whether or not copying is inhibited. The encryption signal SE is received by the decryption circuit 42 of the decryption-signal compression processing circuit block 4 over the signal transmission section 150 **(column 22, lines 56-67 through column 23, lines 1-4).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) apply the teaching of Ezaki into Kori's invention for controlling copying of multimedia data composed of a video signal, an audio signal and so forth, and more particularly to a data processing apparatus wherein a decoder for decoding an electronic watermark (digital watermark) for copy control is built in an encoder for coding a video signal and/or an audio signal in order to protect the video signal and/or the audio signal against alteration **(column 1, lines 7-15 of Ezaki).**

iv. The ordinary skilled person would have been motivated to:

(1) apply the teaching of Ezaki into Kori's invention since from the point of view of protection of the copyright, various attempts have been made to prevent illegal copying of literary works of multimedia data such as, for example, an image signal (or video signal) and an audio signal. It is to be noted that such information may sometimes be hereinafter referred to as contents **(column 1, lines 25-30 of Ezaki).**

b. *Referring to claim 2:*

i. Kori further teaches:

(1) wherein the data signal is either a " No more copy" signal or a "Never copy" signal **[i.e., there are superimposed on the picture data "copy free", specifying that picture or music data recorded on the recording medium or transmitted can be copied, "one copy", specifying that only one copying operation is possible, "no more copy" specifying that data has been copied from the above "one copy" data, or "never copy" specifying that copying cannot be permitted (column 8, lines 45-51)].**

c. *Referring to claim 3:*

i. Kori further teaches:

(1) wherein the digital watermark further contains type data indicating a type of data storage medium on which the encrypted data signal is recorded **[i.e., The copyright information, superimposed on the picture data, may be exemplified by the following copyright control information: That is, there are**

superimposed on the picture data "copy free", specifying that picture or music data recorded on the recording medium or transmitted can be copied, "one copy", specifying that only one copying operation is possible, "no more copy" specifying that data has been copied from the above "one copy" data, or "never copy" specifying that copying cannot be permitted. The reproducing device or the recording device, which has detected this copyright control information, limits reproduction or recording on the picture or music data (column 1, line 60 through column 2, line 6). Furthermore, on the optical disc D, there is recorded the media type information of this optical disc D, along with the above-mentioned picture data or audio data. This media type information is the information specifying whether the optical disc is the read-only ROM disc or a recordable RAM disc (column 2, lines 10-15)].

d. *Referring to claim 4:*

i. Kori further teaches:

(1) a data storage medium having an encrypted data signal as described in claim 1 recorded thereon **[i.e., referring to Figure 4, the optical disc drive 20 includes an optical disc D which is for recording picture data or speech data (column 8, lines 30-33)].**

e. *Referring to claim 5:*

i. Kori further teaches:

(1) further haveing an encrypted first key and an encrypted second key recorded thereon, wherein the first key is used for encrypting the data signal having a superimposed digital watermark, and the second key is used for encrypting the first key **[i.e., referring again to Figure 4, the optical disc drive 20 includes the first CSS encoder 21 and the second CSS encoder 22 to perform encrypting by the so-called contents scramble system (CSS). The first CSS encoder 21 and the second CSS encoder 22 perform encrypting using different algorithms or different encryption keys (column 9, lines 1-5)].**

f. *Referring to claim 6:*

i. Kori teaches:

(1) a reader for reading an encrypted data signal from a data storage medium as described in claim 4 **[i.e., on the optical disc D, there is recorded the media type information of this optical disc D, along with the above-mentioned picture data or audio data. This media type information is the information specifying whether the optical disc is the read-only ROM disc or a recordable RAM disc. From this optical disc D, the above media type information as well as the compressed picture or audio data is read out by the optical disc drive 20 (column 8, lines 55-63)]**;

(2) an encryption state detector for detecting that the encrypted data signal read by the reader is encrypted **[i.e., The optical disc drive 20 includes a first CSS encoder 21 for encrypting the read-out compressed picture and speech data and a second CSS encoder 22 for encrypting the read-out media type information. The first CSS encoder 21 and the second CSS encoder 22 perform encrypting by the so-called contents scramble system (CSS). The first CSS encoder 21 and the second CSS encoder 22 perform encrypting using different algorithms or different encryption keys (column 8, line 64 through column 9, line 5)]**;

(3) a decryption unit for decrypting the encrypted data signal and extracting the data signal with the superimposed digital watermark; a digital watermark decoder for extracting the digital watermark from the data signal decrypted by the decryption unit, and identifying content of the identification data **[i.e., referring to Figure 4, The first CSS decoder 31 and the second CSS decoder 32 perform encryption using different algorithms or different encryption keys in a corresponding manner to the first and second CSS encoders 21 and 22, respectively. Thus, if decryption cannot be effectuated in one of the first or second CSS decoders 31, 32, outputting is halted in its entirety so that no ensuing processing can be performed. The MPEG decoder 33 expands the compressed picture and audio data. The expanded picture data is sent to the watermark (WM) detection/re-encoding unit 35. The expanded speech data is outputted to outside via switch 37 (column 9, lines 50-60)]**; and

(4) a playback controller for comparing a state detected by the encryption state detector and a state indicated by the identification data detected by the digital watermark decoder, and prohibiting playback of the data signal if the states do not match **[i.e., in another aspect, Kori's invention provides a data reproducing apparatus including reproducing means for reproducing data recorded on a recording medium; encryption means for encrypting the data reproduced by the reproducing means and control data relevant at least to copyright control processing of the data, transmission means for transmitting data encrypted by the encrypting means to an external signal processing device, reception means for receiving playback control data transmitted from the external signal processing device, the playback control data being the data transmitted by the transmission means encrypted in a manner different from the encrypting by the encrypting means and processed with copyright control processing, decrypting means for doing decrypting matched to encrypting of the playback control data received by the reception means, and control means for controlling the playback processing of the reproducing means based on the playback control data decrypted by the decrypting means (column 4, lines 7-26)].**

g. *Referring to claim 7:*

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

h. *Referring to claim 8:*

i. This claim has limitations that is similar to those of claims 3 and 6, thus it is rejected with the same rationale applied against claims 3 and 6 above.

i. *Referring to claim 9:*

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above. Futhermore, referring to Figure 5, wherein the VID encoder 41 is fed with the picture data decoded by the MPEG decoder 21 and with the information on the number of passes of the ticket as verified by the ticket verification unit 22 (column 14, lines 10-14).

j. *Referring to claim 13:*

i. Kori teaches:

(1) a digital watermark processor for superimposing to the data signal, as a digital watermark, identification data identifying the data signal as an encrypted signal **[i.e., referring to Figure 4, the watermark (WM) detection/re-encoding unit 35 detects the copyright control information superimposed on the picture data by watermark processing. The detected copyright control information specifies one of "copy free", "one copy", "no more copy" or "never copy", as described above (column 9, line 66 through column 10, line 4). Furthermore, the WM detection unit 61 is fed with picture data expanded by the MPEG decoder 21. The WM detection unit 61 detects (which means identifies) the encrypted key superimposed on the picture data by watermark processing to send the detected encrypted key to the encrypting unit 62. The encrypting unit 62 is fed with the pass information of the ticket from the ticket verification unit 22. The encrypting unit 62 encrypts the ticket pass information using the above-mentioned encrypting key. The encrypted ticket pass information is sent to the VID encoder 41. In addition, the ticket information, encrypted as the VID during the blanking period, is superimposed on the video signals (these are the encrypted signals) (column 16, lines 10-34)];**

(2) an encryption unit for generating an encrypted data signal by encrypting the data signal to which the digital watermark processor superimposed a digital watermark **[i.e., the optical disc drive 20 includes a first CSS encoder 21 for encrypting the read-out compressed picture and speech data and a second CSS encoder 22 for encrypting the read-out media type information. The first CSS encoder 21 and the second CSS encoder 22 perform encrypting by the so-called contents scramble system (CSS). The first CSS encoder 21 and the second CSS encoder 22 perform encrypting using different algorithms or different encryption keys (column 8, line 64 through column 9, line 5)]**; and

(3) a writer for writing the encrypted data signal generated by the encryption unit to the data storage medium **[i.e., on the optical disc D, there is recorded the media type information of this optical disc D, along with**

the above-mentioned picture data or audio data. This media type information is the information specifying whether the optical disc is the read-only ROM disc or a recordable RAM disc, which is writable (column 8, lines 55-60)].

ii. Although Kori transparently and implicitly teaches identification data identifying the data signal as an encrypted signal as mention above, Exaki et al teaches:

(1) The encryption section 142 of the transmission side apparatus 140 encrypts original contents S0 using such a key as described above. The original contents S0 may be, for example, a video signal and/or an audio signal or the like. When the encryption section 142 encrypts the original contents S0, it also encrypts CCI (Copy Control Information) indicative of whether or not copying of an audio signal illustrated in FIG. 2 or a video signal illustrated in FIGS. 3A and 3B is inhibited and places the encrypted CCI into the encrypted signal of the original contents S0. Accordingly, the encryption signal SE includes not only the encrypted original contents S0 but also the encrypted CCI which indicates whether or not copying is inhibited. The encryption signal SE is received by the decryption circuit 42 of the decryption-signal compression processing circuit block 4 over the signal transmission section 150 (column 22, lines 56-67 through column 23, lines 1-4).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) apply the teaching of Ezaki into Kori's invention for controlling copying of multimedia data composed of a video signal, an audio signal and so forth, and more particularly to a data processing apparatus wherein a decoder for decoding an electronic watermark (digital watermark) for copy control is built in an encoder for coding a video signal and/or an audio signal in order to protect the video signal and/or the audio signal against alteration **(column 1, lines 7-15 of Ezaki).**

iv. The ordinary skilled person would have been motivated to:

(1) apply the teaching of Ezaki into Kori's invention since from the point of view of protection of the copyright, various attempts have been made to prevent illegal copying of literary works of multimedia data such as, for example, an

image signal (or video signal) and an audio signal. It is to be noted that such information may sometimes be hereinafter referred to as contents **(column 1, lines 25-30 of Ezaki).**

k. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

l. *Referring to claim 15:*

i. Kori further teaches:

(1) a digital watermark decoder for extracting the digital watermark superimposed to the data signal and detecting the content indicated by the identification data **[i.e., the MPEG decoder 33 expands the compressed picture and audio data. The expanded picture data is sent to the watermark (WM) detection/re-encoding unit 35. The expanded speech data is outputted to outside via switch 37. The medium type decoder decodes the media type information supplied from the second CSS decoder 32 to detect the information on whether the optical disc D reproduced by the optical disc drive 20 is the ROM disc or the RAM disc to send the detected information to the output controller 37 (column 9, lines 57-65)]**; and

(2) a recording controller for permitting recording based on the identification data detected by the digital watermark decoder **[i.e., the output controller 36 performs on/off control of the switches 37, 38 based on the information sent from the media type decoder 34 and from the watermark (WM) detection/re-encoding unit 35. Specifically, if the optical disc D is the ROM disc and the copyright control information is the "no more copy", and if the optical disc D is the RAM disc and the copyright control information is "one copy", the output controller 36 assumes that the data recorded on the optical disc D has been copied illicitly and performs control to turn the switches 37, 38 off (column 10, lines 18-27)].**

m. *Referring to claim 20:*

i. This claim has limitations that is similar to those of claim 13 (3), thus it is rejected with the same rationale applied against claim 13 (3) above.

4. Claims 10-12, 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kori, further in view of Ezaki et al (US 6,721,437 B1), and further in view of Wehrenberg (US 6,523,113 B1).

a. *Referring to claims 10 and 11:*

i. Kori and Ezaki teach all the claimed subject matter as in claim 6 except for:

(1) a first authentication unit; a second authentication unit; wherein the first authentication unit and the second authentication unit communicate through the interface, the first authentication unit verifies if the decoder is a compliant device, and the second authentication unit verifies if the drive device is a compliant device; and the playback controller permits data signal playback when authentication by the first authentication unit and the second authentication unit is successful.

(2) the data storage medium further has recorded thereon a first authentication key and second authentication key used respectively by the first authentication unit and the second authentication unit; the first authentication unit has a first device key assigned specifically to the drive device, and generates a first media authentication key based on the first authentication key, the first device key, and the data storage medium type detected by the type detector, the second authentication unit has a second device key assigned specifically to the decoder, and generates a second media authentication key based on the second authentication key and the second device key, and the first authentication unit and the second authentication unit compare the first media authentication key and the second media authentication key for authentication.

ii. However, Wehrenberg teaches:

(1) referring to Figure 7, the copy system includes a player 310, a computer 300 and a recording device 330. A player 310 includes a CSS authenticator 312 and a DVD disc 320 that contains content that is MPEG compressed,

CSS scrambled and includes an encoded watermark. CSS authenticator 312 allows the content of DVD disc 320 to be played back to computer 300. However, the played back data is still MPEG compressed and includes an encoded watermark. CSS code information is passed along to computer 300 to allow playback of the data. Once CSS authentication 312 has occurred, the data from DVD disc 320 is passed along to decoder 340 of computer 300. Decoder 340 is a single device, such that the elements of the decoder cannot be accessed without a great amount of effort **(column 10, lines 13-42)**.

(2) Knowledge of a "global key" is necessary to perform the authentication and the exchange of the "disc" and "title" keys. The "global key" is incorporated in drives and in CSS compatible host systems in protected modules such that a user cannot easily obtain access to the "global key". The "global key" allows the host to participate in the "authentication" step, which precedes the transfer of the descrambling keys and the scrambled data. Generally, the "global key" is kept confidential among manufacturers to avoid proliferation of the "global key." After the authentication protocol has been completed, drive 14 will read disc 12 and obtain "title keys" from a region of the disc which is not accessible to the host, and pass these keys in encrypted form to host 20. The components of the host system 20, which are CSS compliant, are able to decrypt these keys and use the information to descramble the audio/video data subsequently retrieved from the disc **(column 1, lines 43-60).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the authenticator (in Kori) because with the proliferation of digital recording, the ability to create unauthorized copies of digitally recorded content has become a serious problem for those that have a vested interested in the content. Copyright laws prohibit the unauthorized copying of copyrighted materials. However, copyright laws seldom prevent individuals from unauthorized copying **(column 1, lines 20-26 of Wehrenberg).**

iv. The ordinary skilled person would have been motivated to:

(1) include the authenticator (in Kori) to provide a data reproducing method and apparatus, a data transmitting system, a data transmitting method and a data processing method and apparatus having high security against unauthorized duplication of transmitted or recorded data **(column 3, lines 55-60 of Kori).**

b. *Referring to claims 12 and 18:*

i. These claims have limitations that is similar to those of claim 10, thus they are rejected with the same rationale applied against claim 10 above.

c. *Referring to claim 16:*

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

d. *Referring to claim 17:*

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

e. *Referring to claim 19:*

i. This claim has limitations that is similar to those of claims 5 and 11, thus it is rejected with the same rationale applied against claims 5 and 11 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
April 18, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100